



Arizona Senate Audit

Digital Findings

Presented By Ben Cotton



Arizona Senate Audit

- Withheld Devices and Data
- Cyber Security Issues
- Hardware Configuration Control
- File Deletions
- Failure to Preserve Election Artifacts
- Anonymous Logins
- Listening Ports and Attempted Connections on Bootup
- Internet Connections and History



Arizona Senate Audit

Withheld Devices and Data

- Routers and Network Related Data
- Poll Worker Laptops
- ICX Devices
- ICP Credentials to Validate Configuration Settings or Administrative Settings
- Other Devices Connected to Election Network
 - 192.168.100.1
 - 192.168.100.11



Cyber Security Issues

- Failed to Perform Basic OS Patch Management
- Failed to Update AntiVirus Definitions
- EAC Certification Defense is NOT Valid In View of the Evidence
 - 4 .exe Files Created After Dominion Software Install
 - 45 .exe Files Modified After Dominion Software Install
 - 377 .dll Files Created After Dominion Software Install
 - 1053 .dll Files Modified After Dominion Software Install
- Log Management - Failed to Preserve Security Logs
- Credential Management – Shared Accounts and Common Passwords
- Failed to Establish and Monitor Host Baseline



Hardware Configuration Issues

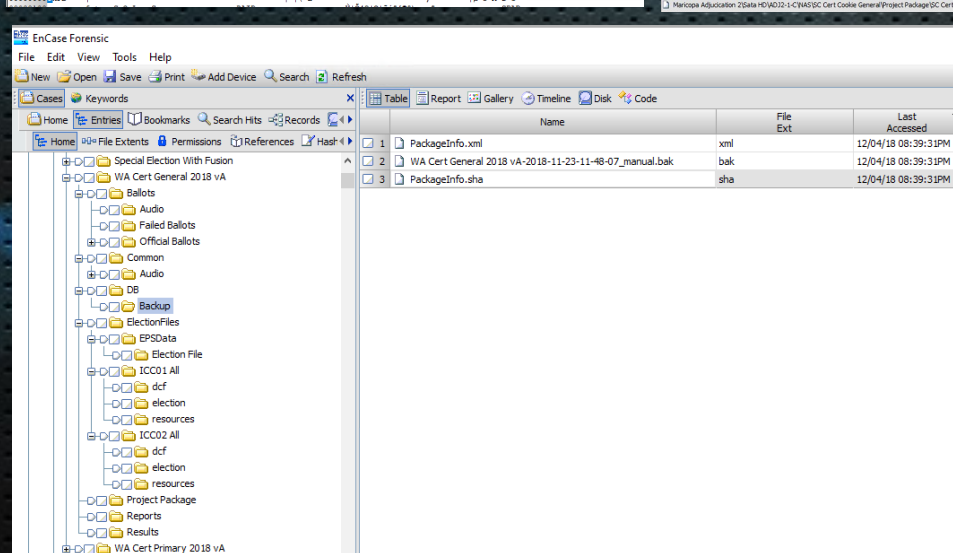
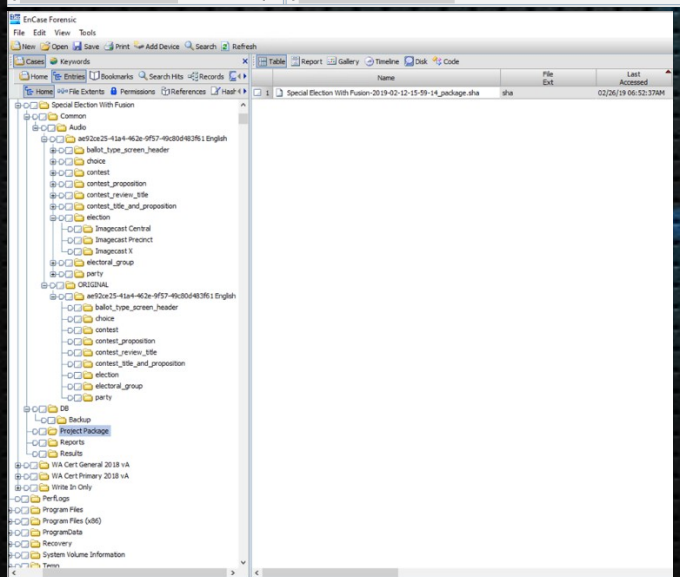
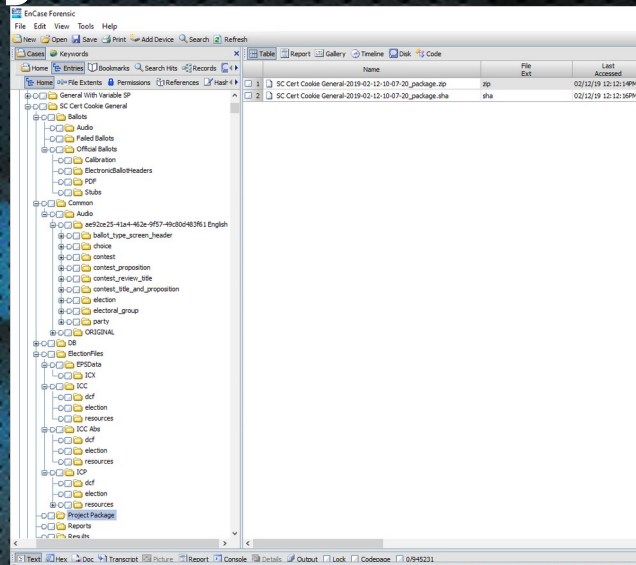
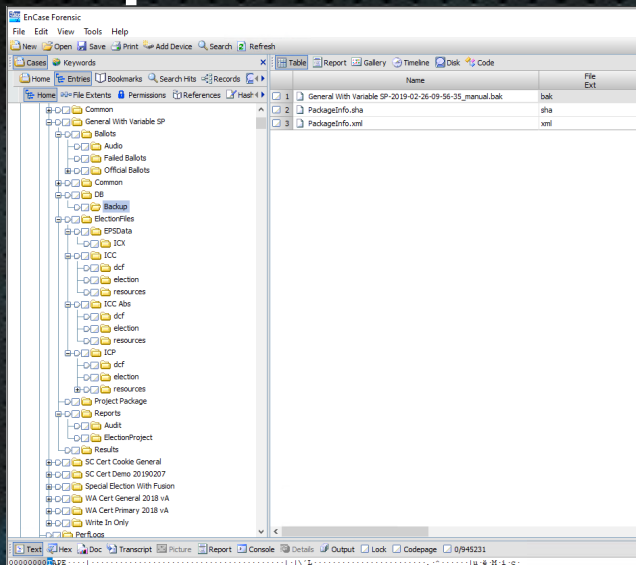
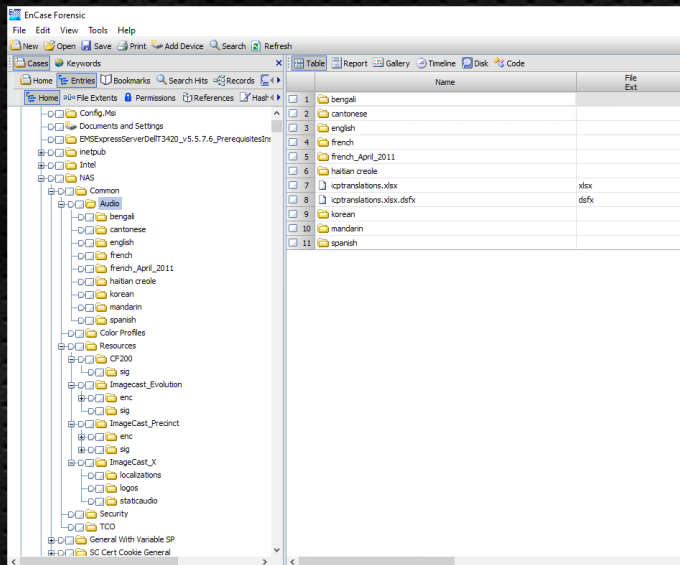
- Dual Boot Configuration Discovered on Adjudication 02 Endpoint
 - Two Hard Drives Internal to System
 - Both Drives Bootable to Different Configurations
- Clearly Not an Approved Configuration
- 2nd Hard Drive Contained Non-Maricopa County Data





Arizona Senate Audit

Non-Maricopa County Data





Arizona Senate Audit

File Deletions From EMS C:\ Drive

- 865 directories and 85,673 Election Related Files (scanned ballots, .dvd files, slog.txt files, etc) Deleted Between 10/28/20 and 11/05/20

The screenshot displays the EnCase Forensic interface. The main window shows a list of files with columns for Name, File Ext, Last Accessed, File Created, Last Written, Entry Modified, File Acquired, and Logical Size. The files are organized into batches (Batch130 to Batch147) and images. The search results pane on the right shows a list of files with checkboxes for selection and filters for search descriptions and selected files only.

Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size
73778 06033_00153_000152.tf	tf	11/05/20 11:33:00AM	11/05/20 11:33:00AM	11/05/20 11:33:00AM	03/04/21 10:32:24AM	04/23/2...	377,032 Flk
73779 06033_00153_000153.tf	tf	11/05/20 11:33:00AM	11/05/20 11:33:00AM	11/05/20 11:33:00AM	03/04/21 10:32:24AM	04/23/2...	372,148 Flk
73780 06033_00153_000155.tf	tf	11/05/20 11:33:02AM	11/05/20 11:33:02AM	11/05/20 11:33:02AM	03/04/21 10:32:24AM	04/23/2...	384,390 Flk
73781 06033_00153_000154.tf	tf	11/05/20 11:33:02AM	11/05/20 11:33:02AM	11/05/20 11:33:02AM	03/04/21 10:32:24AM	04/23/2...	373,300 Flk
73782 06033_00153_000156.tf	tf	11/05/20 11:33:04AM	11/05/20 11:33:04AM	11/05/20 11:33:04AM	03/04/21 10:32:24AM	04/23/2...	374,571 Flk
73783 06033_00153_000157.tf	tf	11/05/20 11:33:04AM	11/05/20 11:33:04AM	11/05/20 11:33:04AM	03/04/21 10:32:24AM	04/23/2...	383,620 Flk
73784 06033_00153_000158.tf	tf	11/05/20 11:33:04AM	11/05/20 11:33:04AM	11/05/20 11:33:04AM	03/04/21 10:32:24AM	04/23/2...	371,545 Flk
73785 06033_00153_000160.tf	tf	11/05/20 11:33:06AM	11/05/20 11:33:06AM	11/05/20 11:33:06AM	03/04/21 10:32:24AM	04/23/2...	371,142 Flk
73786 06033_00153_000159.tf	tf	11/05/20 11:33:06AM	11/05/20 11:33:06AM	11/05/20 11:33:06AM	03/04/21 10:32:24AM	04/23/2...	369,937 Flk
73787 06033_00153_000161.tf	tf	11/05/20 11:33:08AM	11/05/20 11:33:08AM	11/05/20 11:33:08AM	03/04/21 10:32:24AM	04/23/2...	380,413 Flk
73788 06033_00153_000162.tf	tf	11/05/20 11:33:08AM	11/05/20 11:33:08AM	11/05/20 11:33:08AM	03/04/21 10:32:24AM	04/23/2...	371,851 Flk
73789 06033_00153_000163.tf	tf	11/05/20 11:33:10AM	11/05/20 11:33:10AM	11/05/20 11:33:10AM	03/04/21 10:32:24AM	04/23/2...	363,797 Flk
73790 06033_00153_000164.tf	tf	11/05/20 11:33:10AM	11/05/20 11:33:10AM	11/05/20 11:33:10AM	03/04/21 10:32:24AM	04/23/2...	372,631 Flk
73791 06033_00153_000165.tf	tf	11/05/20 11:33:12AM	11/05/20 11:33:12AM	11/05/20 11:33:12AM	03/04/21 10:32:24AM	04/23/2...	377,774 Flk
73792 06033_00153_000166.tf	tf	11/05/20 11:33:12AM	11/05/20 11:33:12AM	11/05/20 11:33:12AM	03/04/21 10:32:24AM	04/23/2...	380,825 Flk
73793 06033_00153_000167.tf	tf	11/05/20 11:33:14AM	11/05/20 11:33:14AM	11/05/20 11:33:14AM	03/04/21 10:32:24AM	04/23/2...	389,046 Flk
73794 06033_00153_000168.tf	tf	11/05/20 11:33:14AM	11/05/20 11:33:14AM	11/05/20 11:33:14AM	03/04/21 10:32:24AM	04/23/2...	365,468 Flk
73795 06033_00153_000170.tf	tf	11/05/20 11:33:16AM	11/05/20 11:33:16AM	11/05/20 11:33:16AM	03/04/21 10:32:24AM	04/23/2...	373,666 Flk
73796 06033_00153_000169.tf	tf	11/05/20 11:33:16AM	11/05/20 11:33:16AM	11/05/20 11:33:16AM	03/04/21 10:32:24AM	04/23/2...	370,260 Flk
73797 06033_00153_000171.tf	tf	11/05/20 11:33:18AM	11/05/20 11:33:18AM	11/05/20 11:33:18AM	03/04/21 10:32:24AM	04/23/2...	371,586 Flk



Arizona Senate Audit

File Deletions EMS D:\ Drive

- 9,571 Directories and 1,064,746 Election Related Files Were Deleted Between 11/01/20 and 03/16/21

The screenshot displays the EnCase Forensic interface. The top menu bar includes File, Edit, View, Tools, and Help. Below the menu is a toolbar with icons for New, Open, Save, Print, Add Device, Search, Refresh, and Query. The main window is divided into several panes. On the left, the 'Cases' pane shows a tree view with 'Home', 'Entries', 'Bookmarks', 'Search Hits', 'Records', 'Permissions', 'References', and 'Hash'. The 'Entries' pane shows a list of files with columns for Name, File Ext, Last Accessed, File Created, Last Written, Entry Modified, File Acquired, Logical Size, Description, and File Type. The 'Table' pane shows a list of files with columns for Name, File Ext, Last Accessed, File Created, Last Written, Entry Modified, File Acquired, Logical Size, Description, and File Type. The 'Text' pane shows a hex dump of the selected file. The 'Console' pane shows a list of search results. The 'Output' pane shows a list of search results. The 'Codepage' pane shows a list of search results. The 'EnScript' pane shows a list of search results. The 'Filters' pane shows a list of search results. The 'Conditions' pane shows a list of search results. The 'Display' pane shows a list of search results. The 'Queries' pane shows a list of search results. The 'Text Styles' pane shows a list of search results. The status bar at the bottom indicates the current file path: Maricopa EMS D Drive\Lost Files\Batch035\Images\03032_00035_000028.tif (PS 2700169664 LS 2700169664 CL 337521208 SO 000 FO 0 LE 0).

Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size	Description	File Type
03032_00035_000024.tif	tif	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM		367,830	File, Deleted, Archive	TIFF Image
03032_00035_000028.tif	tif	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM		368,468	File, Deleted, Archive	TIFF Image
03032_00035_000032.tif	tif	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM		370,959	File, Deleted, Archive	TIFF Image
03032_00035_000036.tif	tif	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM	11/01/20 11:15:17AM		363,031	File, Deleted, Archive	TIFF Image



Arizona Senate Audit

Deleted Files – HiPro 1

- 304 Directories and 59,387 Files Containing Election Data Deleted From the HiPro Scanner 1 on 3 March 2021

The screenshot displays the EnCase Forensic application window. The left pane shows a directory tree with folders labeled Batch013 through Batch033. The main pane shows a table of deleted files. The table has columns for Name, File Ext, Last Accessed, File Created, Last Written, Entry Modified, File Acquired, Logical Size, and a status column. The files listed are .tif files with names starting with 03031_00022_000165.tif through 03031_00022_000190.tif. The status column shows 'F' for files and 'E' for entries.

Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size	
159134 03031_00022_000165.tif	tif	03/03/21 01:04:09PM	03/03/21 01:04:09PM	11/01/20 11:44:41AM	11/01/20 11:44:41AM	04/24/2...	417,449	F
159135 03031_00022_000172.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:22AM	11/01/20 11:42:22AM	04/24/2...	428,130	F
159136 03031_00022_000173.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:22AM	11/01/20 11:42:22AM	04/24/2...	422,211	F
159137 03031_00022_000174.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:23AM	11/01/20 11:42:23AM	04/24/2...	465,514	F
159138 03031_00022_000175.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:23AM	11/01/20 11:42:23AM	04/24/2...	425,169	F
159139 03031_00022_000176.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:24AM	11/01/20 11:42:24AM	04/24/2...	421,977	F
159140 03031_00022_000177.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:24AM	11/01/20 11:42:24AM	04/24/2...	425,173	F
159141 03031_00022_000178.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:24AM	11/01/20 11:42:24AM	04/24/2...	417,201	F
159142 03031_00022_000179.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:25AM	11/01/20 11:42:25AM	04/24/2...	418,388	F
159143 03031_00022_000180.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:25AM	11/01/20 11:42:25AM	04/24/2...	421,539	F
159144 03031_00022_000181.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:26AM	11/01/20 11:42:26AM	04/24/2...	422,688	F
159145 03031_00022_000182.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:26AM	11/01/20 11:42:26AM	04/24/2...	423,214	F
159146 03031_00022_000183.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:27AM	11/01/20 11:42:27AM	04/24/2...	426,149	F
159147 03031_00022_000184.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:27AM	11/01/20 11:42:27AM	04/24/2...	355,785	F
159148 03031_00022_000185.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:27AM	11/01/20 11:42:27AM	04/24/2...	420,395	F
159149 03031_00022_000186.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:28AM	11/01/20 11:42:28AM	04/24/2...	424,135	F
159150 03031_00022_000187.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:28AM	11/01/20 11:42:28AM	04/24/2...	430,635	F
159151 03031_00022_000188.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:29AM	11/01/20 11:42:29AM	04/24/2...	423,214	F
159152 03031_00022_000189.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:29AM	11/01/20 11:42:29AM	04/24/2...	390,763	F
159153 03031_00022_000190.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:29AM	11/01/20 11:42:29AM	04/24/2...	446,688	F
159154 03031_00022_000191.tif	tif	03/03/21 01:04:10PM	03/03/21 01:04:10PM	11/01/20 11:42:29AM	11/01/20 11:42:29AM	04/24/2...	425,767	F



Arizona Senate Audit

Deleted Files – HiPro 3

- 1,016 Directories and 196,463 Files Containing Election Data Deleted From the HiPro Scanner 3 on 3 March 2021

The screenshot shows the EnCase Forensic interface with a list of deleted files. The left pane shows a directory tree with 'HiPro3-C' selected. The main pane displays a table of files with columns for Name, File Ext, Last Accessed, File Created, Last Written, Entry Modified, File Acquired, Logical Size, Description, File Type, and File Category.

	Name	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size	Description	File Type	File Category
274	03033_00001_000186.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:37AM	11/01/20 09:28:37AM	04/24/21 11:45:57PM	355,949	File, Deleted, Archive	TIFF Image	Picture
275	03033_00001_000187.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:38AM	11/01/20 09:28:38AM	04/24/21 11:45:57PM	365,470	File, Deleted, Archive	TIFF Image	Picture
276	03033_00001_000188.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:38AM	11/01/20 09:28:38AM	04/24/21 11:45:57PM	371,471	File, Deleted, Archive	TIFF Image	Picture
277	03033_00001_000189.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:39AM	11/01/20 09:28:39AM	04/24/21 11:45:57PM	363,757	File, Deleted, Archive	TIFF Image	Picture
278	03033_00001_000190.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:39AM	11/01/20 09:28:39AM	04/24/21 11:45:57PM	374,396	File, Deleted, Archive	TIFF Image	Picture
279	03033_00001_000191.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:40AM	11/01/20 09:28:40AM	04/24/21 11:45:57PM	408,977	File, Deleted, Archive	TIFF Image	Picture
280	03033_00001_000192.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:40AM	11/01/20 09:28:40AM	04/24/21 11:45:57PM	412,578	File, Deleted, Archive	TIFF Image	Picture
281	03033_00001_000193.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:40AM	11/01/20 09:28:40AM	04/24/21 11:45:57PM	403,155	File, Deleted, Archive	TIFF Image	Picture
282	03033_00001_000194.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:41AM	11/01/20 09:28:41AM	04/24/21 11:45:57PM	381,415	File, Deleted, Archive	TIFF Image	Picture
283	03033_00001_000195.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:41AM	11/01/20 09:28:41AM	04/24/21 11:45:57PM	397,916	File, Deleted, Archive	TIFF Image	Picture
284	03033_00001_000196.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:42AM	11/01/20 09:28:42AM	04/24/21 11:45:57PM	398,939	File, Deleted, Archive	TIFF Image	Picture
285	03033_00001_000197.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:42AM	11/01/20 09:28:42AM	04/24/21 11:45:57PM	375,327	File, Deleted, Archive	TIFF Image	Picture
286	03033_00001_000198.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:42AM	11/01/20 09:28:42AM	04/24/21 11:45:57PM	355,994	File, Deleted, Archive	TIFF Image	Picture
287	03033_00001_000199.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:43AM	11/01/20 09:28:43AM	04/24/21 11:45:57PM	364,655	File, Deleted, Archive	TIFF Image	Picture
288	03033_00001_000200.tif	tif	03/03/21 01:27:11PM	03/03/21 01:27:11PM	11/01/20 09:28:43AM	11/01/20 09:28:43AM	04/24/21 11:45:57PM	388,092	File, Deleted, Archive	TIFF Image	Picture
289	04003_00001_000001.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:20PM	11/12/20 06:19:20PM	04/24/21 11:45:57PM	398,553	File, Deleted, Archive	TIFF Image	Picture
290	04003_00001_000002.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:21PM	11/12/20 06:19:21PM	04/24/21 11:45:57PM	397,240	File, Deleted, Archive	TIFF Image	Picture
291	04003_00001_000003.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:21PM	11/12/20 06:19:21PM	04/24/21 11:45:57PM	387,120	File, Deleted, Archive	TIFF Image	Picture
292	04003_00001_000004.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:21PM	11/12/20 06:19:21PM	04/24/21 11:45:57PM	378,679	File, Deleted, Archive	TIFF Image	Picture
293	04003_00001_000005.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:22PM	11/12/20 06:19:22PM	04/24/21 11:45:57PM	429,814	File, Deleted, Archive	TIFF Image	Picture
294	04003_00001_000006.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:22PM	11/12/20 06:19:22PM	04/24/21 11:45:57PM	384,623	File, Deleted, Archive	TIFF Image	Picture
295	04003_00001_000007.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:23PM	11/12/20 06:19:23PM	04/24/21 11:45:57PM	388,865	File, Deleted, Archive	TIFF Image	Picture
296	04003_00001_000008.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:23PM	11/12/20 06:19:23PM	04/24/21 11:45:57PM	398,151	File, Deleted, Archive	TIFF Image	Picture
297	04003_00001_000009.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:24PM	11/12/20 06:19:24PM	04/24/21 11:45:57PM	389,036	File, Deleted, Archive	TIFF Image	Picture
298	04003_00001_000010.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:24PM	11/12/20 06:19:24PM	04/24/21 11:45:57PM	390,045	File, Deleted, Archive	TIFF Image	Picture
299	04003_00001_000011.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:24PM	11/12/20 06:19:24PM	04/24/21 11:45:57PM	384,230	File, Deleted, Archive	TIFF Image	Picture
300	04003_00001_000012.tif	tif	03/03/21 01:26:56PM	03/03/21 01:26:56PM	11/12/20 06:19:25PM	11/12/20 06:19:25PM	04/24/21 11:45:57PM	413,517	File, Deleted, Archive	TIFF Image	Picture



Arizona Senate Audit

Deleted Files – HiPro 4

- 981 Directories and 191,295 Files Containing Election Data Deleted From the HiPro Scanner 4 on 3 March 2021

The screenshot displays the EnCase Forensic application window. The left sidebar shows a tree view of file batches, with 'Batch038' selected. The main pane shows a table of file entries. The table has columns for File ID, File Ext, Last Accessed, File Created, Last Written, Entry Modified, File Acquired, Logical Size, Description, File Type, File Category, Signature, and Is Deleted. The entries are sorted by File ID, showing a range from 191259 to 191295. Each entry is marked as 'Deleted' in the 'Is Deleted' column.

File ID	File Ext	Last Accessed	File Created	Last Written	Entry Modified	File Acquired	Logical Size	Description	File Type	File Category	Signature	Is Deleted
191259	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:10AM	10/28/20 10:17:10AM	04/25/21 03:44:21PM	387,719	File, Deleted, Archive	TIFF Image	Picture		*
191260	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:10AM	10/28/20 10:17:10AM	04/25/21 03:44:21PM	390,600	File, Deleted, Archive	TIFF Image	Picture		*
191261	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:11AM	10/28/20 10:17:11AM	04/25/21 03:44:21PM	383,262	File, Deleted, Archive	TIFF Image	Picture		*
191262	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:11AM	10/28/20 10:17:11AM	04/25/21 03:44:21PM	392,783	File, Deleted, Archive	TIFF Image	Picture		*
191263	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:12AM	10/28/20 10:17:12AM	04/25/21 03:44:21PM	390,433	File, Deleted, Archive	TIFF Image	Picture		*
191264	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:12AM	10/28/20 10:17:12AM	04/25/21 03:44:21PM	413,147	File, Deleted, Archive	TIFF Image	Picture		*
191265	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:13AM	10/28/20 10:17:13AM	04/25/21 03:44:21PM	382,284	File, Deleted, Archive	TIFF Image	Picture		*
191266	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:13AM	10/28/20 10:17:13AM	04/25/21 03:44:21PM	390,709	File, Deleted, Archive	TIFF Image	Picture		*
191267	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:14AM	10/28/20 10:17:14AM	04/25/21 03:44:21PM	414,506	File, Deleted, Archive	TIFF Image	Picture		*
191268	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:14AM	10/28/20 10:17:14AM	04/25/21 03:44:21PM	414,805	File, Deleted, Archive	TIFF Image	Picture		*
191269	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:14AM	10/28/20 10:17:14AM	04/25/21 03:44:21PM	392,080	File, Deleted, Archive	TIFF Image	Picture		*
191270	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:15AM	10/28/20 10:17:15AM	04/25/21 03:44:21PM	390,199	File, Deleted, Archive	TIFF Image	Picture		*
191271	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:15AM	10/28/20 10:17:15AM	04/25/21 03:44:21PM	375,588	File, Deleted, Archive	TIFF Image	Picture		*
191272	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:16AM	10/28/20 10:17:16AM	04/25/21 03:44:21PM	392,352	File, Deleted, Archive	TIFF Image	Picture		*
191273	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:16AM	10/28/20 10:17:16AM	04/25/21 03:44:21PM	390,075	File, Deleted, Archive	TIFF Image	Picture		*
191274	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:16AM	10/28/20 10:17:16AM	04/25/21 03:44:21PM	402,080	File, Deleted, Archive	TIFF Image	Picture		*
191275	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:17AM	10/28/20 10:17:17AM	04/25/21 03:44:21PM	390,751	File, Deleted, Archive	TIFF Image	Picture		*
191276	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:17AM	10/28/20 10:17:17AM	04/25/21 03:44:21PM	404,390	File, Deleted, Archive	TIFF Image	Picture		*
191277	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:18AM	10/28/20 10:17:18AM	04/25/21 03:44:21PM	390,721	File, Deleted, Archive	TIFF Image	Picture		*
191278	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:18AM	10/28/20 10:17:18AM	04/25/21 03:44:21PM	388,107	File, Deleted, Archive	TIFF Image	Picture		*
191279	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:19AM	10/28/20 10:17:19AM	04/25/21 03:44:21PM	413,468	File, Deleted, Archive	TIFF Image	Picture		*
191280	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:19AM	10/28/20 10:17:19AM	04/25/21 03:44:21PM	392,154	File, Deleted, Archive	TIFF Image	Picture		*
191281	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:19AM	10/28/20 10:17:19AM	04/25/21 03:44:21PM	390,951	File, Deleted, Archive	TIFF Image	Picture		*
191282	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:20AM	10/28/20 10:17:20AM	04/25/21 03:44:21PM	362,766	File, Deleted, Archive	TIFF Image	Picture		*
191283	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:21AM	10/28/20 10:17:21AM	04/25/21 03:44:21PM	374,380	File, Deleted, Archive	TIFF Image	Picture		*
191284	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:21AM	10/28/20 10:17:21AM	04/25/21 03:44:21PM	388,673	File, Deleted, Archive	TIFF Image	Picture		*
191285	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:22AM	10/28/20 10:17:22AM	04/25/21 03:44:21PM	391,803	File, Deleted, Archive	TIFF Image	Picture		*
191286	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:22AM	10/28/20 10:17:22AM	04/25/21 03:44:21PM	383,037	File, Deleted, Archive	TIFF Image	Picture		*
191287	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:22AM	10/28/20 10:17:22AM	04/25/21 03:44:21PM	413,681	File, Deleted, Archive	TIFF Image	Picture		*
191288	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:23AM	10/28/20 10:17:23AM	04/25/21 03:44:21PM	390,709	File, Deleted, Archive	TIFF Image	Picture		*
191289	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:23AM	10/28/20 10:17:23AM	04/25/21 03:44:21PM	370,453	File, Deleted, Archive	TIFF Image	Picture		*
191290	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:24AM	10/28/20 10:17:24AM	04/25/21 03:44:21PM	402,494	File, Deleted, Archive	TIFF Image	Picture		*
191291	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:24AM	10/28/20 10:17:24AM	04/25/21 03:44:21PM	384,332	File, Deleted, Archive	TIFF Image	Picture		*
191292	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:24AM	10/28/20 10:17:24AM	04/25/21 03:44:21PM	391,785	File, Deleted, Archive	TIFF Image	Picture		*
191293	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:43AM	10/28/20 10:17:43AM	04/25/21 03:44:21PM	377,820	File, Deleted, Archive	TIFF Image	Picture		*
191294	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:43AM	10/28/20 10:17:43AM	04/25/21 03:44:21PM	398,708	File, Deleted, Archive	TIFF Image	Picture		*
191295	tf	03/03/21 02:44:33PM	03/03/21 02:44:33PM	10/28/20 10:17:20AM	10/28/20 10:17:20AM	04/25/21 03:44:21PM	381,020	File, Deleted, Archive	TIFF Image	Picture		*



Arizona Senate Audit

Failure to Preserve Operating System Logs

- Logs Produced by Maricopa County Did Not Contain the Windows Security Logs
- Security Logs Set to Maintain 20MB of Data
- Oldest Date in Windows Security Log on EMS was 2/5/21
 - Did not Cover Election Time Period
- Clear Intentional Overwriting of the Security Logs by the EMSADMIN Account
 - 2/11/2021 – 462 Log Entries Overwritten
 - 3/3/2021 – 37,686 Log Entries Overwritten
 - 4/12/2021 – 330 Log Entries Overwritten



General Election Results Purged from EMS

- 2/1/2021 – SQL Logs Indicate That the RTRAdmin Account Purged the General Election Results from the Database
- Windows Access Logs Don't have a Corresponding Entry

2...	4DA1500D-7B7D-4437-88EC-492C79DAF75B	Admin	User initiates the Close Project activity	LD01		2021-01-21 09:22:47.563
2...	76B314A4-600D-4F8C-AF5D-818D448F5203	RTRAdmin	Project 20201103 General opened	LD01		2021-02-01 17:14:21.550
2...	AB0EF054-F8C5-4217-A0B4-5BC20566F1AE	RTRAdmin	User initiates the Result Files activity	LD01		2021-02-01 17:14:21.567
2...	36615BC3-F4F9-4E6D-92A0-560C2DCF645F	RTRAdmin	User initiates the OnPurgeResults activity	LD01		2021-02-01 17:14:47.363
2...	D839A42C-16A2-47C7-8066-CAA584EBB531	RTRAdmin	User initiates generation of password.	LD01		2021-02-01 17:15:01.160
2...	EDAC3600-0978-4EED-82FA-447F8858B793	RTRAdmin	PurgeResultsCommand (execution duration: 76478ms):All result files from database were deleted.	LD01	NULL	2021-02-01 17:16:27.810
2...	39B7BDFD-BE64-4501-9BFF-CCCECF9E2A0	RTRAdmin	PurgeResultsCommand (execution duration: 288779ms):The result files database, result files and images from NAS were deleted. Purging of results has finished successfully.	LD01	NULL	2021-02-01 17:20:00.097
2...	036292E2-0F66-4F30-9308-6E1D55377B97	RTRAdmin	User initiates the Election Summary Report activity	LD01		2021-02-01 17:21:55.173



Arizona Senate Audit

Anonymous Logins

- Some Anonymous Login Activity is Normal
- Atypical Anonymous Logins Were Discovered

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

Impersonation Level: Impersonation

New Logon:

- Security ID: ANONYMOUS LOGON
- Account Name: ANONYMOUS LOGON
- Account Domain: NT AUTHORITY
- Logon ID: 0x8AFF32
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x0
- Process Name: -

Network Information:

- Workstation Name: DESKTOP-██████
- Source Network Address: 192.168.██████
- Source Port: 61322

Detailed Authentication Information:

- Logon Process: NtLmSsp
- Authentication Package: NTLM

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 8/27/2021 11:02:02 AM

Task Category: Logon

Keywords: Audit Success

Computer: ██████████

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

Impersonation Level: Impersonation

New Logon:

- Security ID: ANONYMOUS LOGON
- Account Name: ANONYMOUS LOGON
- Account Domain: NT AUTHORITY
- Logon ID: 0x2ACBE
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x0
- Process Name: -

Network Information:

- Workstation Name: -
- Source Network Address: -
- Source Port: -

Detailed Authentication Information:

- Logon Process: NtLmSsp
- Authentication Package: NTLM

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

OpCode: Info

More Information: [Event Log Online Help](#)

Logged: 2/10/2021 4:07:19 PM

Task Category: Logon

Keywords: Audit Success

Computer: EMSSERVER



Arizona Senate Audit

EMS Listening Ports

- Analysis Discovered 59 Ports That Were Open on the EMS Server at Boot
- Unexpected High Port Listening Activity by Standard Windows Processes (winit.exe, dns.exe, dhcpserver)
- IPV6 Enabled
- Terminal Services are Enabled
- Remote Access is Enabled

Arizona Senate Audit EMS Network Connection Attempts on Boot

Process Name	Process File Path	Process ID	Dest IP	Dest Port	Whois
system	system	4	192.168.100.1	445	N/A Local Lan
avastsvc.exe	c:\program files\avast software\ avast business\avastsvc.exe	320	23.194.212.49	80	Akamai
avastsvc.exe	c:\program files\avast software\ avast business\avastsvc.exe	320	23.194.212.56	80	Akamai
svchost.exe	c:\windows\system32\svchost.exe	988	8.252.68.126	80	Level 3 Parent, LLC
svchost.exe	c:\windows\system32\svchost.exe	988	72.21.81.240	80	Edgecast
svchost.exe	c:\windows\system32\svchost.exe	988	13.107.4.50	80	Microsoft
svchost.exe	c:\windows\system32\svchost.exe	988	23.194.212.104	80	Akamai
svchost.exe	c:\windows\system32\svchost.exe	988	8.240.49.254	80	Level 3 Parent, LLC
svchost.exe	c:\windows\system32\svchost.exe	988	8.252.36.126	80	Level 3 Parent, LLC
svchost.exe	c:\windows\system32\svchost.exe	1272	64.4.54.254	443	Microsoft
svchost.exe	c:\windows\system32\svchost.exe	1272	52.137.106.217	443	Microsoft
svchost.exe	c:\windows\system32\svchost.exe	1272	20.72.205.209	443	Microsoft
jusched.exe	c:\program files (x86)\common files\java\java update\jusched.exe	4680	184.86.196.202	443	Akamai
avastemupdate. exe	c:\program files\avast software\ avast business\ avastemupdate.exe	8092	104.99.72.230	80	Akamai



Arizona Senate Audit

Internet History and Connections

- Both Maricopa County Audits did Not Find Any Internet History
- Significant Internet History Recovered from Unallocated Space
 - EMS Server
 - EMS Client Workstations
 - Adjudication Workstations
 - REWEB 1601
 - REGIS 1202



Arizona Senate Audit

EMS Server

Date Visited [UTC]	Date Visited [Local]	Visits	URL
2021-02-02 00:17:30.906	2021-02-01 17:17:30.906	1	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker
2021-02-02 00:17:33.935	2021-02-01 17:17:33.935	2	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker



Arizona Senate Audit

EMS Client 1

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
02/07/2020 20:02:19	02/07/2020 13:02:19	2	http://www.bing.com/search?q=192.138.100.11&src=IE-SearchBox&FORM=IE11SR&pc=EUPP_	
02/22/2021 23:08:13	02/22/2021 16:08:13	5	https://go.microsoft.com/fwlink/?LinkId=838604	emsadmin01
02/07/2020 20:00:53	02/07/2020 13:00:53	2	https://go.microsoft.com/fwlink/p/?LinkId=255141	emsadmin01

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
10/30/2019 17:00:49	10/30/2019 10:00:49	2	http://192.168.100.11/p_preference.html	emsadmin01
10/30/2019 17:00:54	10/30/2019 10:00:54	2	http://192.168.100.11/m_network.html	emsadmin01
10/30/2019 17:00:58	10/30/2019 10:00:58	2	http://192.168.100.11/m_network_tcpip.html	emsadmin01
10/30/2019 17:01:46	10/30/2019 10:01:46	2	http://192.168.100.11/m_system.html	emsadmin01
10/30/2019 17:01:50	10/30/2019 10:01:50	2	http://192.168.100.11/m_security.html	emsadmin01
10/30/2019 17:02:02	10/30/2019 10:02:02	2	http://192.168.100.11/m_network_ethernet.html	emsadmin01
10/30/2019 17:02:46	10/30/2019 10:02:46	2	http://192.168.100.11/m_network_ipv4.html	emsadmin01
10/30/2019 17:03:38	10/30/2019 10:03:38	2	http://192.168.100.11/m_network_snmp.html	emsadmin01
10/30/2019 17:03:46	10/30/2019 10:03:46	2	http://192.168.100.11/m_network_port.html	emsadmin01
10/30/2019 17:03:51	10/30/2019 10:03:51	2	http://192.168.100.11/m_network_port_edit.html	emsadmin01
10/30/2019 17:04:00	10/30/2019 10:04:00	2	http://192.168.100.11/m_network_starttime.html	emsadmin01
10/30/2019 17:04:21	10/30/2019 10:04:21	2	http://192.168.100.11/m_network_wirelesslan.html	emsadmin01



Arizona Senate Audit

EMS Client 3

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:01	08/06/2019 09:26:01	2	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:01	08/06/2019 09:26:01	2	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:13	08/06/2019 09:26:13	3	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:27	08/06/2019 09:26:27	3	http://192.168.100.11/checkLogin.cgi	emsadmin01
08/06/2019 16:26:27	08/06/2019 09:26:27	3	http://192.168.100.11/portal_top.html	emsadmin01
02/04/2021 00:36:19	02/03/2021 17:36:19	6	https://go.microsoft.com/fwlink/?LinkId=838604	emsadmin03



Arizona Senate Audit

REWEB1601

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://global.fncstatic.com/static/isa/core.js?v=20200116173547	
01/17/2020 17:16:09	01/17/2020 10:16:09	4	https://static.foxnews.com/static/orion/scripts/core/ag.core.js?v=20200116173547	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://static.foxnews.com/static/orion/html/video/iframe/vod.html?v=20200116173547	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://static.foxnews.com/static/orion/html/video/iframe/vod.html?v=20200116173547	serveradmin
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://static.foxnews.com/static/orion/styles/img/core/s/bg/close.svg	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://static.foxnews.com/static/orion/scripts/core/components/loader.newsletter.xdcomm.js?v...	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://ajax.googleapis.com/ajax/libs/jquery/1.11.2/jquery.min.js	
01/17/2020 17:16:09	01/17/2020 10:16:09	2	https://my.foxnews.com/js/bootstrap.js	
01/17/2020 17:16:08	01/17/2020 10:16:08	4	https://static.foxnews.com/static/orion/scripts/core/templates/ag.app.js?v=20200116173547	
01/17/2020 17:16:08	01/17/2020 10:16:08	2	https://static.foxnews.com/static/orion/scripts/core/ag.core.js	
01/17/2020 17:16:08	01/17/2020 10:16:08	2	https://static.foxnews.com/static/orion/scripts/core/templates/app/iframe.html?v=20200116173...	
01/17/2020 17:16:08	01/17/2020 10:16:08	2	https://static.foxnews.com/static/orion/scripts/core/templates/app/iframe.html?v=20200116173...	serveradmin



Arizona Senate Audit

REGIS 1202

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
11/25/2019 14:50:28	11/25/2019 07:50:28	3	https://156.42.40.59:1311/OMSALogin?msgStatus=null	serveradmin
11/25/2019 14:50:27	11/25/2019 07:50:27	5	https://156.42.40.59:1311/LoginServlet?flag=true&managedws=true	serveradmin
11/25/2019 14:49:58	11/25/2019 07:49:58	2	https://156.42.40.59:1311/OMSALogin?msgStatus=false&PasswordEmpty=false	serveradmin
11/25/2019 14:49:57	11/25/2019 07:49:57	2	https://156.42.40.59:1311/omalogin.html?msgStatus=false&manageDWS=true&PasswordEmpt...	serveradmin
11/25/2019 14:48:37	11/25/2019 07:48:37	3	https://156.42.40.59:1311/OMSALogin	serveradmin
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/js/gnavbar.js	
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/js/Clarity.js	
11/25/2019 14:48:29	11/25/2019 07:48:29	3	https://156.42.40.59:1311/oma/js/prototype.js	
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/css/masthead.css	
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/css/common.css	
11/25/2019 14:48:29	11/25/2019 07:48:29	2	https://156.42.40.59:1311/oma/js/favicon.js	
11/25/2019 14:48:13	11/25/2019 07:48:13	2	https://156.42.40.59:1311/OMSALogin	serveradmin
11/25/2019 14:48:13	11/25/2019 07:48:13	2	https://156.42.40.59:1311/OMSALogin	serveradmin



Questions?